НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

3. *Insikt Group, Recorded Future*. 2024 Malicious Infrastructure Report: Threat Intelligence Report. — Recorded Future, 2025.
4. *USTelecom*. Botnet and IoT Security Trends 2024: Industry Report. — USTelecom, 2024. — URL: https://ustelecom.org/wp-content/uploads/2024/03/USTelecom-Botnet-and-Security-Trends-2024.pdf.
5. *Imperva Threat Research, Thales*. 2025 Bad Bot Report: The Rapid Rise of Bots and The Unseen Risk for Business: Annual Report. — Imperva, 2025. — URL: https://www.imperva.com/resources/resource-library/reports/2025-bad-bot-report/.
6. *SecurityOnline Info*. The Largest DDoS Attack in History: Cloudflare Fights Back. — https://securityonline.info/the-largest-ddos-attack-in-history-cloudflare-fights-back/, 2025.
7. *Sandbox Interactive, Albion Online Forum*. Resolved: Ongoing DDoS Attack & Compensation (Forum Post). — https://forum.albiononline.com/index.php/Thread/214699-Resolved-Ongoing-DDoS-Attack-Compensation/#post1442554, 2025.

Ключові слова: ханіпот, високоінтерактивний, nginx, ботнет, виявлення атак, zero-day, мережевий відбиток, емуляція, кібербезпека, автоматизований трафік, вебсервер, розвідувальні дані, ddos-атака, маскування, шкідливе пз, віртуалізація, журналювання, мережева інфраструктура, критична інфраструктура, сигнатури.
Keywords: honeypot, high-interaction, nginx, botnet, attack detection, zero-day, network fingerprint, emulation, cybersecurity, automated traffic, web server, threat intelligence, ddos attack, deception, malware, virtualization, logging, network infrastructure, critical infrastructure, signatures

МІЖНАБОРНЕ ТЕСТУВАННЯ МЕТОДУ KNN+TF-IDF У ЗАДАЧІ ВИЯВЛЕННЯ ІН'ЄКЦІЙНИХ АТАК У ВЕБ-ЗАПИТАХ

Коробейнікова Тетяна
к.т.н., доцент, доцент кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка»
Кравчук Назар
аспірант, асистент кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка»

У сучасних вебзастосунках, що характеризуються великою кількістю динамічних інтеграцій і складною структурою даних, ризик появи ін'єкційних атак (SQLi, XSS, ін'єкцій команд) залишається одним із ключових викликів для систем кіберзахисту. Традиційні сигнатурні рішення IDS/WAF часто не здатні ефективно розпізнавати обфусковані або нові варіанти атак, тоді як моделі глибинного навчання вимагають значних обчислювальних ресурсів і не завжди забезпечують прозорість прийняття рішень. У попередній роботі нами було показано, що поєднання алгоритму k-найближчих сусідів (KNN) із TF-IDF-представленням текстових навантажень і додатковими структурно-статистичними ознаками дозволяє досягти високої ефективності виявлення ін'єкцій (до 99,77% точності та F_1=0,998) при низьких ресурсних витратах.

У цьому дослідженні ми зосередили увагу на міжнаборному тестуванні (Cross-Dataset Evaluation) для оцінювання узагальнювальної здатності вдосконаленої моделі KNN+TF-IDF. Головною метою є перевірка стійкості моделі до зміни домену даних — тобто її здатності коректно класифікувати ін'єкційні атаки з наборів даних, що не використовувалися під час навчання.

Експериментальне оцінювання проводилося на трьох відкритих наборах даних: HttpParamsDataset (навчальний корпус), SQLi/XSS Dataset та OS Command Injection Dataset. Для базової моделі використовувалася лише TF-IDF-векторизація тексту, тоді як вдосконалена модель включала сім додаткових числових ознак: довжину навантаження, кількість цифр, кількість великих літер, щільність спеціальних символів, ентропію, індикатор логічних тавтологій і сигнатури системних команд.

Таблиця 1 подає порівняльні результати базової та вдосконаленої моделей на невідомих наборах даних. Як і очікувалося, точність знижується, коли моделі, навчені на HttpParamsDataset, стикаються з новими структурами навантажень. Однак розширений набір ознак суттєво пом'якшує це погіршення, забезпечуючи покращення як точності Accuracy, так і зваженого показника $F_{1\text{-weighted}}$.

Таблиця 1 - Результати узагальнення між наборами даних (Cross-Dataset Generalization Results)

Dataset	k	Metric	Accuracy	$F_{1-weighted}$
SQLi/XSS (Baseline)	5	Cosine	0.6475	0.6431
SQLi/XSS (Improved)	5	Cosine	0.7674	0.7688
Command Injection (Baseline)	5	Cosine	0.8527	0.8305
Command Injection (Improved)	5	Cosine	0.8741	0.8533

Список літератури

1. Таченко І. А. Огляд сучасного стану питання в галузі оцінювання ризиків мережевої безпеки / І. А. Таченко, Т. І. Коробейнікова, С. М. Захарченко // Scientific Collection «InterConf», (84): with the Proceedings of the 5th International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects» (November 7-8, 2021). Rome, Italy: Dana, 2021. 478 p. – С. 417-432.
2. ISO/IEC 27005:2018. Information technology — Security techniques — Information security risk management. International Organization for Standardization.
3. NIST SP 800-37 Rev. 2. (2018). Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. National Institute of Standards and Technology.
4. ENISA. (2020–2024). Threat Landscape Reports. European Union Agency for Cybersecurity.

Ключові слова: ін'єкційні атаки, виявлення атак, KNN, TF-IDF.
Keywords: injection attacks, attack detection, KNN, TF-IDF.

ЗМІСТ